http://ansinet.com/itj

ITJ

ISSN 1812-5638

INFORMATION TECHNOLOGY JOURNAL

ANSInet
Asian Network for Scientific Information
308 Lasani Town, Sargodha Road, Faisalabad - Pakistan

Information Technology Journal 12 (15): 3447-3451, 2013
ISSN 1812-5638 / DOI: 10.3923/itj.2013.3447.3451

Hybrid Attacks on Complex Networks in Redundancy and Workload View

Xu Ye and Xu Ying
School of Information and Science Engineering, Shenyang Ligong University,
110159, Shenyang, China

Abstract: Cascading failure of complex networks has become a research focus recently. For a better view of networks properties, BA scale-free network is generated and a router level Internet topology is measured. Attacks experiments are conducted on these network samples so that there is a possibility for us to have a better understanding what hurts a network most and how to improve its corresponding robustness. The attacks experiments are mainly conducted on networks with parameters of different redundancies, different workloads and different attacks. Finally, ideas to improve network robustness are proposed.

Key words: Complex networks, cascading failure, robustness, redundancy

INTRODUCTION

The networks in modern world are getting more and more complex and security of corresponding networks has become a research focus. In Internet, social networks, transportation networks, biological networks, technology networks and many other networks in real world, one or a few nodes or edges sometimes fail due to random failure or target attacks. The failure, however, usually is propagated from the node where the failure occurs towards its neighbors and therefore results in the failure of some other nodes in a certain possibility. This will sometimes lead to a chain reaction, resulting in failures of a considerable part or even the whole part of the networks. The phenomenon found here is called cascading failure (Barabasi, 2002). For the safety and reliability of the Internet and other networks in real world, it is necessary for us to focus on studies of the occurrence, prevention and control of the cascading failure in complex networks.

Researchers generally agree that complex networks are robust and fragile in complex networks view (Watts and Strogatz, 1998; Barabasi and Albert, 1999; Doyle *et al*., 2005). Once a fragile node in networks fails, its negative effects will propagated and result in the entire collapse of the whole networks. The Internet, for example, virus attacks on some routers may lead to its overload and forced routing packets occur. The overload may affect other routers and eventually led to the failure propagation avalanche effect. Studies have found (Barabasi and Albert, 1999; Doyle *et al*., 2005) the scale-free network topology the network is close to many large-scale networks in real world so that attacks on scale-free networks is convenient for us to study robustness properties of complex networks.

EXPERIMENT NETWORKS SAMPLES

Models of scale-free networks: Scale-free network model (Moreno *et al*., 2002), also known as BA scale-free network model has properties of degree power-law distribution which is close to those of some large-scale networks in real world such as Internet, WWW and so on. Two simple rules are set for generating a scale-free network and they are: (1) Given an initial networks with a small amount of nodes, for next each stage a new node with some (random) links are added to this networks, (2) New edges are linked to the existed nodes by a preferential rule which is the probability of linking to a selected node is proportional to the degree of this node (Bollobas and Riordan, 2003).

The following graph is the generated graph of scale-free model:

Generation of scale-free networks: According to the BA scale-free network model, we set a network with 3 initial node connecting with each other so that the established initial network has a degree distribution value of 2. With preferential attachment rules, a scale-free networks containing 500 nodes is generated. Define the capacity (carry maximum load) of node (i) is proportional to its initial load (Moreno *et al*., 2002) L_i:

$$C_i = (1+\alpha)L_i \quad (1)$$

Corresponding Author: Xu Ye, School of Information and Science Engineering, Shenyang Ligong University, 110159, Shenyang, China

where, $\alpha \geq 0$ is a constant that is the expandable load capacity of the node and $\alpha = 0$ means there is no expandable load in the network. The initial load of the node (L) is defined as:

$$L = b * K(\alpha + \beta) \quad (2)$$

where, b is a multiplying factor and α is a coefficient index. The greater a node's degree is, the more load ability the node is. When $\alpha = 1$, the system performance reaches best. β is the attenuation coefficient, it shows that a node's load capacity is proportional but not fully proportional to the degree of the node.

Measuring Internet topology: Testing samples in this paper were generated from what was measured at twenty-one CAIDA (CAIDA, 2013) monitors. With the twenty-one measured data, we first gather them together to form a complete testing sample. Then, for a better view and analysis, we made several incomplete testing samples and they are sample (1) comprising data from only one monitors (arin monitor) and sample (2) from two monitors (arin, b-root), till sample (20) from twenty monitors.

Then we eventually get twenty-one testing samples together with the complete testing sample. To main reason to generate these twenty-one samples is to avoid the sampling bias in the large extent. Though the problem of sampling bias is not the main topic of the paper, we still made our efforts to reduce the effect of the sampling bias by increasing sampling nodes and this is why we select as many as twenty-one CAIDA monitors.

However, there is still no good approach to completely solve the problem of sampling bias except trying to include more sampling nodes at present, so we could not prove how much sampling bias is solved by using the twenty-one-monitor sample and. The key point is, the more monitors we use, the less the sampling bias would be. So the complete sample (the twenty-one monitor sample) is the primary testing sample in this paper and the a 500 node network is drawn from the Internet measuring results.

MATHEMATICAL DESCRIPTION OF CASCADING FAILURES AND ROBUSTNESS IN COMPLEX NETWORKS

The purpose that we study the robustness of complex networks (Albert *et al*., 2000; Pastor-Satorras *et al*., 2001) is to improve their abilities against attacks. When a cascading failure occurs in complex networks, a robustness measure is used to identify how much the network is damaged. Network robustness (G) is defined as the ratio of the largest connected subgraph in network after a failure propagation over the initial network size (Moreno *et al*., 2002):

$$G = \frac{N'}{N} \quad (3)$$

where, N is the number of nodes in a lagest connected subgraph before the network cascading failures occurred and N' is that after failures. At $G \to 0$, it means that the network is completely collapsed since there is no large connected subgraph remained in the network. In real networks, however, a network would be regarded as a crash much before $G \to 0$, usually we take it as a collapse when $G < 0.1$.

ATTACK EXPERIMENTS AND SIMULATIONS

Simulation experiments mainly focus on random attacks and target attacks on both the generated scale-free networks and the measured Internet topology.

Parameters settings: θ $(0 \leq \theta \leq 1)$ (theta) is the node redundancy factor, $\theta = 0$ means there is no extension in the network, $\theta = 1$ means that the capacity of the network is doubled.

ω $(0 \leq \omega \leq 1)$ is the current load of a node in network, when $\omega = 0$ it means a empty network with no loads. $\theta = 1$ means the current load reaches its maximum value.

τ (tao) is the type of attacks, $\tau = 0$ is completely target attack, while $\tau = 1$ means totally random attack.

Redundancy experiments against attacks: The networks robustness experiments against random and target attacks with different redundancies are illustrated as follows, in which the blue curves are for Internet and the red ones for scale-free networks. In the experiments, we set $\tau = 0$ for target attacks and $\tau = 1$ for random attacks, $\omega = 0.8$ for both networks with 80% of workloads. In the meanwhile, θ is set to increase from 0 to 1 with a step of 0.3 in Fig. 2a and a step of 0.5 in Fig. 2b so as to have a close view of behaviors of redundancy networks against different attacks.

From the Fig. 2a experiments against target attacks, at $\theta = 0$, we see both networks collapse (identified as $G < 0.1$) sharply; At $\theta = 0.3$, we see that Internet would breakdown when 8% nodes are destructed and for scale-free networks it's 3%; Similarly at $\theta = 0.6$ and at $\theta = 0.9$, a destruction of 20% nodes would result in a 50% breakdown of Internet and that for the BA scale-free network is 20%.

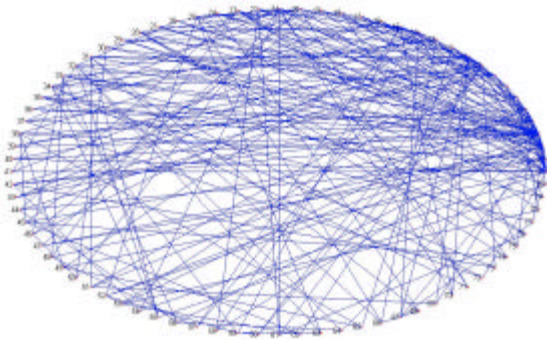

Fig. 1: Three examples of 80 nodes scale-free networks

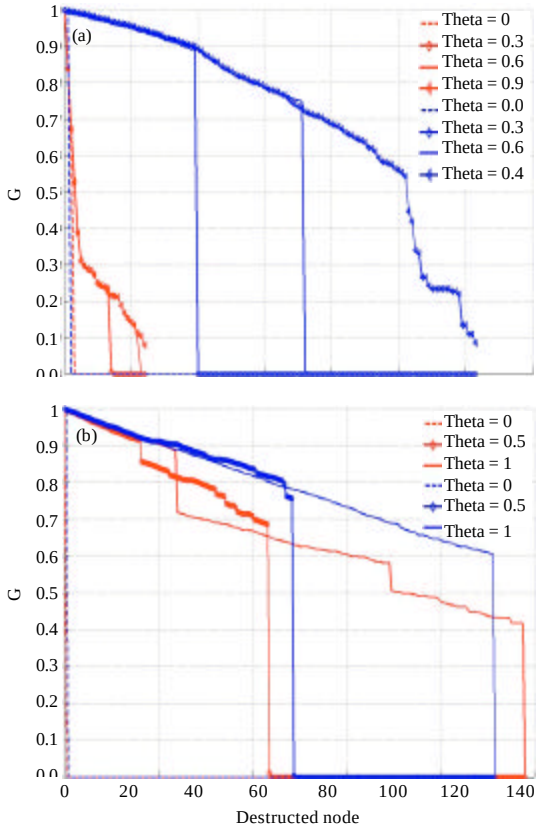

Fig. 2(a-b): Networks robustness experiments against random and target attacks with different redundancies, (a) Two networks against target attacks with $\tau = 0$ and w = 0.8 and (b) Two networks against random attacks with $\tau = 1$ and w = 0.8

From the Fig. 2b experiments against random attacks, we see both networks collapse (identified as G<0.1) sharply at $\theta = 0$; at $\theta = 0.5$, we see that Internet would breakdown when 25% nodes are destructed and for scale-free networks it's 22%; at $\theta = 1$, a destruction of 45% nodes would result in a 50% breakdown of Internet and that for the BA scale-free network is 48%.

From both Fig. 2a and b we see that both networks are robust against random attacks but fragile under target attacks. Under target attacks, Internet seems to be more robust than the scale-free networks, the reason might be that compared with the pure scale-free networks, Internet is not so much clustered so that the target attacks would not give so much influence on the whole networks. And for random attacks, both Internet and scale-free networks seem to be similar to each other. Most of all, experiments show that redundancy would make both the networks much stronger against both random and target attacks. The redundancy is a good choice to improve networks' robustness in case of ignoring costs.

Workload experiments against attacks: The networks robustness experiments against random and target attacks with different workloads are illustrated as follows, in which the blue curves are for Internet and the red ones for scale-free networks. In the experiments, we set $\tau = 0$ for target attacks and $\tau = 1$ for random attacks, $\theta = 0$ for both networks with no redundancies. In the meanwhile, ω is set to increase from 0 to 1 with a step of 0.5 in Fg. 3a and a step of 0.3 in Fig. 3b so as to have a close view of behaviors of workload networks against different attacks.

From the Fig. 3a experiments against target attacks, at w = 0, a destruction of 24% nodes would result in a breakdown of Internet and that for the BA scale-free network is 6%; at w = 0.5, we see that Internet would breakdown when 14% nodes are destructed and for scale-free networks it's 4% and finally at w = 1, any attacks would result in a quick collapse.

From the Fig. 3b experiments against random attacks, we see both networks collapse (identified as G<0.1) sharply at w = 0.9 and this is mainly due to the almost full load of networks and any destruction of nodes could make failure be propagated throughout the networks. At w = 0.6, we see that Internet would breakdown when 15% nodes are destructed and for scale-free networks it's 18%; And at w = 0.3, a destruction of 67% nodes would result in a breakdown of Internet and that for the BA scale-free network is 90%.

From both Fig. 3a and b we see that both networks are robust against random attacks but fragile under target attacks. Under same attacks, the more workload a network has, the more fragile the network is. What make us surprise is that scale-free networks seem to be more robust than Internet under random attacks. The reason might be that Internet is not so much the kind of pure

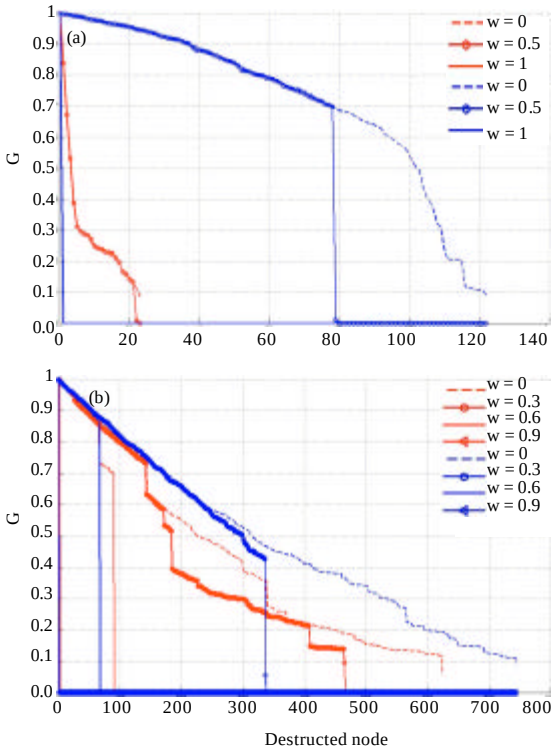

Fig. 3(a-b): Networks robustness experiments against random and target attacks with different workloads, (a) Two networks against target attacks withτ = 0 and θ=0 and (b) Two networks against random attacks withτ = 1 and θ = 0

scale-free networks and has not the absolute power-law distribution in degree. So the robustness properties in topology complying with power-law distribution are not so much clear in Internet.

Most of all, experiments show that the workload would make both the networks much worse in robustness against both random and target attacks. Finding a way to reduce workloads of networks is a good way to improve networks' robustness.

Hybrid attacks experiments: The networks robustness experiments against hybrid attacks with some workloads and no redundancies are illustrated as follows, in which the blue curves are for Internet and the red ones for scale-free networks. In the experiments, we set θ = 0 meaning there is no redundancies and ω = 0.3 meaning the networks are lightly loaded. Most importantly, τ is set to increase from 0 to 1 with a step of 0.5 in Fig. 4 so as to have a better view of behaviors of networks against different and hybrid attacks.

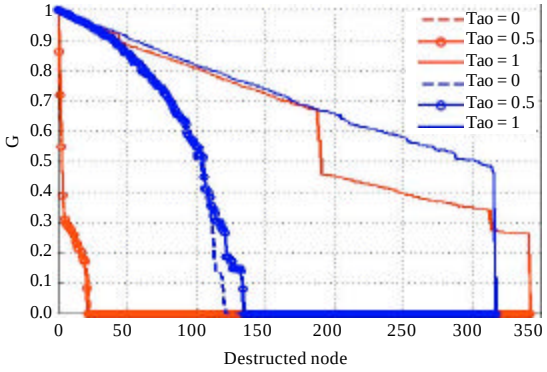

Fig. 4: Networks robustness experiments against hybrid attacks with no redundancies and light workloads at θ=0 and w=0.3

From Fig. 4 we see that the random attacks (τ = 1) cause similar destructions in both networks. And the result of hybrid attacks (τ = 0.5) is close to that of target attacks (τ = 0) although one attack is a kind of hybrid attack and the other is absolute target attack. The reason might lie in that a slice of target attack would destruct some nodes with very high links which would cause a great hurt to the network topology. So a possible of target attack at τ = 0.5 also causes large quantities of harm to both networks. Here we find that target attacks, though in minor extent, would be the major reason for the collapse of a target networks.

OVERALL ANALYSES

From the above experiments, we find what hurts a network most is the destruction of nodes with many links in target or hybrid attacks. For Internet, it seems to be better in robustness than absolute scale-free networks under target attacks. However, both Internet and scale-free networks are quite good against random attacks.

Most importantly, an increase of redundancy and a decrease of workload would largely influence the robustness of Internet and scale-free networks. The cost, such as the maintenance or generation cost of a network, however, would increase sharply if more redundancy is set in a network.

CONCLUSIONS

With simulation experiments exerted on samples networks including a measured Internet and a generated scale-free network, it's found that both networks are robust under random attacks. While in target attacks or

hybrid attacks, their robustness is weakened although Internet is a little better than scale-free networks. A way to improve robustness of both networks is given, that is to improve the redundancies and decrease their workload, respectively. The increase of redundancy, however, would cause a sharp increase of cost in maintaining target networks.

ACKNOWLEDGMENT

The authors would like to thank for the support by the Natural Science Foundation of China under Grant 61373159. The authors also give thanks for the Shenyang Natural Science Foundation under Grant F13-316-1-22.

REFERENCES

Albert, R., H. Jeong and A.L. Barabasi, 2000. Error and attack tolerance of complex networks. Nature, 406: 378-381.

Barabasi, A.L. and R. Albert, 1999. Emergence of scaling in random networks. J. Sci., 286: 509-512.

Barabasi, A.L., 2002. The New Science of Networks. Persus Publishing, Massachusetts, pp: 127-151.

Bollobas, B. and O. Riordan, 2003. Mathematical Results on Scale-Free Random Graphs. In: Handbook of Graphs and Networks: From the Genome to the Internet, Bornholdt, S. and H.G. Schuster (Eds.). Wiley-VCH, Berlin, pp: 1-34.

CAIDA, 2013. Skitter. The Cooperative Association for Internet Data Analysis. http://www.caida.org/tools /measurement/skitter/.

Doyle, J.C., D.L. Alderson, L. Li, S. Low and M. Roughan *et al*., 2005. The robust yet fragile nature of the internet. Proc. Natl. Acad. Sci. USA., 102: 14497-14502.

Moreno, Y., J.B. Gomez and A.F. Pacheco, 2002. Instability of scale-free networks under node-breaking avalanches. Europhys. Lett., 58: 630-636.

Moreno, Y., R. Pastor-Satorras, A. Vazquez and A. Vespignani, 2002. Critical load and congestion instabilities in scale-free networks. Europhys. Lett., 62: 292-298.

Pastor-Satorras, R., A. Vazquez and A. Vespignani, 2001. Dynamical and correlation properries of the internet. Phys. Rev. Lett., Vol. 87. 10.1103/PhysRevLett.87.258701

Watts, D.J. and S.H. Strogatz, 1998. Collective dynamics of small-world networks. Lett. Nat., 393: 440-442.